REMARKS

By this response, claims 1-58 and 90-101 are pending. Also, claims 1, 25, 58, 90, 98 and 101 are amended while 2-24, 26-57, 91-97, 99 and 100 remain as originally presented before substantive examination. Claims 59-89 remain withdrawn as they did upon the filing of a response to the restriction requirement. In general, amendments to claims 1, 90 and 98 relate to the anticipation rejection while those to 25, 58 and 101 relate to antecedent basis issues.

Substantively, the Examiner rejects all claims as anticipated by Chang et al., U.S. 6,157,953. In general, Chang concerns itself with system administrators and their ability to effectively "manag[e] software applications and services ***from a central location*** in a computer network." *Emphasis Added, col. 5, ll. 14-15.* In all embodiments, the central location resides on a "server side" of the network, separate and distinct from the ultimate end-users of the network. As borne out in Figure 2, for example, Chang teaches a "server-side configuration 200" having sections 202 and 204 representing "an administrative side" and "network servers, or service hosts," respectively. *Col. 5, l. 67 - col. 6, l. 2.* However, end users are "[n]ot shown" in the figure and, as distinguished from the server-side, exist "on client machines which can typically access network servers 206 [of the server-side] to provide services or for running applications, or performing other network operations." *Col. 6, ll. 2-5.*

To tightly control access of the software applications and authenticate a system administrator's right to manipulate software on the server-side of the network, Chang contemplates an authentication process from a single point-of-control, or central location, as described with regard to Figures 8a and 8b at *col. 12, l. 59, et. seq.*

With more specificity, Chang's authentication process begins at step 802 with an administrator pointing the "the browser host (i.e. administration console 216 of FIG. 2) to a URL of the management console host." At step 804, "the administrator/user is challenged for a user name and password for access to the management console program on the console host. At step 806 the management console accepts the user name and password entered in step 804 and the user is authenticated." *Col. 13, ll. 3-7.* At step 808, the administrator selects services of the various hosts they want to manage. In steps 810, 812 and 814, authentication of the administrator occurs. If authentication is ultimately successful, "the management console program on the console host," e.g., the central location, enables the administrator to "perform management operations on the selected service or services from the browser [216] as shown at step 816 at which point the enforcement process is complete." *Col. 13, ll. 58-62.* ***In other words, an administrator logs on and becomes authenticated for various service hosts all while being physically located at the centrally-located, web browser host 216.*** They then perform necessary operations for the service hosts after authentication is complete.

Bear in mind, Chang attempts to overcome prior art problems (*Col. 2, ll. 26-42*) where multiple system administrators, each with varying degrees of authority, need to perform many operations, functions, routines, etc. at multiple locations, including routinely having to "re-authenticate every time" they sign on to a service host, especially in networks where the multiple "service hosts are not in communication with each other." *Col. 2, ll. 54-56.* As Chang further describes it, this is "inefficient and repetitive." *Col. 2, l. 45.*

In contrast to the instant invention: 1) Chang requires an administrator to logon and become authenticated from a single point-of-control, e.g., the "central location" of the web browser host 216; 2) Chang never addresses the interaction of the ultimate end-users of the network, only system administrators; and 3) Chang completely and utterly avoids digital identities of the end-users and how these and the end-users interact with other end-users. To this end, the Applicant requests reconsideration of the claims.

More specifically, claim 1 requires a database having a vault for storing a user object. In turn, the user object has a safe object which contains "at least one profile accessed and administered exclusively by the user at the exclusion of the system administrator." Chang, however, never discusses the ultimate end-users and all embodiments contemplate at least one system administrator having access to perform various operations on a server-side of a network.

Further, the claim requires each profile to include digital identity information from the user and be "operable to be shared with other users having other profiles accessible and administered exclusively by the other users, the sharing occurring exclusively upon initiation by the user." Nowhere does Chang mention the interaction between various end-users, let alone those sharing profiles that are accessible and administered exclusively by the end-users. To the extent Chang's system administrator might be considered "a user," Chang never mentions or otherwise intimates that various users can "share profiles" with one another. The Applicant submits Chang does not then anticipate. Bear in mind, one reason for the Applicant's invention stems from a desire to safely and continually share identity information between multiple users without continually needing to re-enter such information. Also, an underlying "important design goal" of the invention is allowing a "user 1002 control over access to identity information" *Applicant's Specification, p. 24, ll. 23-24*; and a user "can always revoke or change access to his or her identity data" *Id. at ll. 24-25*; as well as being able to "revoke access" to other users. *Id. at ll. 28.*

Still further, claim 1 requires "access rights" in the vault being granted to "a system administrator." On the other hand, users have "exclusive" administration of their own profiles, especially at the exclusion of the system administrator. This is supported in the specification wherein "the administrator 1000 has full administrative rights to the Vault, [a]s indicated by an arrow 1006 from the administrator 1000 to the end user 1002 . . . [and] end users have full access control over their respective Safes [in the vault]." *Applicant's Specification, p. 25, ll. 23-28.* Chang, however, never contemplates such scenarios.

Claim 90 requires a vault "having access rights granted to one or more system administrators including management of one or more accounts of end users" and one or more safes of digital identities in the vault having "access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators." In other words, without restricting the claim scope beyond the words expressly recited, administrators have access rights to vaults and to the management of the accounts of end users. End-users have exclusive access rights to their digital identities in the vault, yet obtained these rights via their accounts, in turn, managed by the administrator. In still other words, end users have access to the substance of their digital identities while administrators give the end users their ability to get to the substance. In contrast, Chang does not mention accounts of end users nor of the end-user/administrator relationship outlined herein. Support for this amendment is shown in the Applicant's Figure 10, for example, and attendant written description.

Claim 98 requires access rights to the vault be given to system administrators while access rights to the digital identity profiles, stored in the vault, be given to end users exclusively. Chang does not mention digital identity profiles anywhere. Chang simply mentions passwords and user names. Also, claim 98 requires the location of the end users be remote from the vault. Chang, conversely, teaches all operations at "a central location."

The entirety of the dependent claims are submitted as being patentable because of their dependence on one of claims 1, 90 or 98 discussed above. Additional reasons of patentability can be given but are being held in abeyance in anticipation of a Notice of Allowance.

Consequently, the Applicant submits that all claims are in a condition for allowance and requests a timely Notice of Allowance to be issued for same. ***To the extent any fees are due, the undersigned authorizes the deduction from Deposit Account No. 11-0978.***

Finally, the Applicant attaches herewith (Exhibit 1) a previously filed Revocation of Prior Power of Attorney and Appointment of New Power of Attorney document and

requests such be entered. The document was first filed in September, 2004 along with a Change of Correspondence Address form (PTO/SB/122). To the undersigned's knowledge, the Patent Office has still not entered this information despite an indication of reception in the form of a September 29, 2004 date stamp on the King & Schickli, PLLC, postcard. ***Also, the new attorney docket number is 1363-006.***

Respectfully submitted,

KING & SCHICKLI, PLLC

Michael T. Sanderson
Registration No, 43,082

247 North Broadway
Lexington, Kentucky 40507
Phone: (859) 252-0889
Fax: (859) 252-0779

Certificate of Mailing
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: MAIL STOP AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on Feb. 24 2005
Date 2-24-05 Carolina Perdomo